AMENDMENTS TO THE SPECIFICATION:

Please amend the paragraph on page 6, beginning at line 15 as follows:

Computer 2 is arranged to support a service provider, typically an enterprise, for the provision of services to a client via the internet 3. Computer 2 incorporates a webserver 11 for providing web access to computer 2 for web clients, for example computer 1, as is well known to a person skilled in the art. In addition to a network protocol stack 12, computer 2 also includes a digital credential management system [[13]]14 for handling trust related processes, such as the management of large numbers of heterogeneous credentials in real time, as described below.

Please amend the paragraph on page 7, beginning at line 23 as follows:

The validation checking of digital identity certificates associated with a session for the purposes of providing a service is defined as the user login phase. For this purpose the digital credential management system 14 incorporates a login service module 15, as shown in figure 2, that interacts with a session manager module 16 to create a new session object that is associated with a secure session, for its whole lifetime. The session object associates extra users' information to their session, for example bank statements associated to a user.

Please amend the paragraph on page 8, beginning at line 1 as follows:

The login service module [[16]]15 retrieves the user's identity certificate from the web server 11 (used to establish the SSL session) and sends the certificate to a credential validation server module 17 for validation and trust management purposes.

Please amend the paragraph on page 8, beginning at line 6 as follows:

The credentials validation server module 17 executes a two-phase control on the digital credential. First it performs "classic" verification tasks, like integrity and validation path checks. It interacts with external entities such as CA, OCSP and CVSP to check if the credential is still valid. OCSP

and CVSP responders perform basic validation tasks on-line. Second, the module 17 determines the trustworthiness of the credential against explicit enterprise policies, for example checking explicit constraints on the validation path, on the issuer of the credentials, on the context in which the credential has been [[send]]sent.

Please amend the paragraph on page 11, beginning at line 11 as follows:

The user context manager module 20 supplies to a digital credentials usage monitoring service module 23 updated sets of active credentials (i.e. credentials that are currently used and enabled in a user context area), and digital credential usage monitoring service monitoring 23 executes the request of enabling/disabling credentials depending on trust and business management decisions.

Please amend the paragraph on page 11, beginning at line 28 as follows:

The user context gateway 24 acts as a gateway in the following cases; (i) when the user context manager module 20 sends to the digital credentials usage monitoring service module 23 an updated list of the digital credentials involved in active users' sessions; and (ii) when the digital credentials usage monitoring service module 23 asks the user context manager module [[30]]20 to enable/disable digital credentials, depending on trust and business management decisions.

Abstract:

Please replace the current Abstract with the following replacement/new Abstract